

PATENT

Atty. Dkt. No. YOR920030570US1

REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application are unpatentable or obvious under the provisions 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-17 AND 23-30 UNDER 35 U.S.C. § 103

The Examiner rejected claims 1-17 and 23-30 as being unpatentable over the Lachman, III et. al patent application (U.S. Patent Application Publication No. 2002/0166063, published November 7, 2002, hereinafter "Lachman") in view of the Nakae et al. patent application (U.S. Patent Application Publication No. 2004/0172557, published September 2, 2004, hereinafter "Nakae") and further in view of the Gong et al. patent (U.S. Patent No. 7,076,801, issued July 11, 2006, hereinafter referred to as "Gong"). In response, the Applicants have amended independent claim 1 in order to more clearly recite aspects of the invention. Claims 23-30 have been cancelled without prejudice. Applicants do not concede that the subject matter encompassed by claims 23-30 is not patentable over the art cited by the Examiner; rather, claims 23-30 were cancelled solely to facilitate expeditious prosecution of the pending claims. Applicants respectfully reserve the right to pursue claims, including the subject matter encompassed by cancelled claims 23-30 and additional claims, in one or more continuing applications.

In particular, the Examiner's attention is respectfully directed to the fact that Lachman, Nakae, and Gong, singly or in any permissible combination, fail to disclose or suggest incrementing a counter that tracks a total number of times that a server has been victim of a security assault and automatically creating a new server instance with a new server configuration if the value of the counter does not exceed a maximum limit, where the new server configuration is selected from a table comprising a plurality of new server configurations, such that the particular configuration of the new server configuration depends on the total number of times that the server has been victim of a security assault (i.e., as indicated by the value of the counter), as recited in amended independent claim 1.

PATENT

Atty. Dkt. No. YOR920030570US1

The Examiner acknowledges in the Office Action that "Lachman ... does not disclose ... wherein said new server instance is selected from a table comprising a plurality of new server configurations, said new server configuration being associated in said table with said value of said counter" (Office action, Page 3). Moreover, Lachman fails to teach the selection of a specific remedy (e.g., new server configuration) based on a total number of times that a server has been attacked. At best, Lachman teaches that an individual attack can be detected when a network load exceeds a threshold (Lachman, paragraph 0102). This is not the same as tracking a total number of times that a particular server has been attacked, as claimed by the Applicants. The Examiner submits, however, that Nakae bridges this gap in the teachings of Lachman. The Applicants respectfully disagree.

Nakae, by contrast, teaches taking a specific action (i.e., luring an IP packet causing a DoS attack into a decoy unit) when a confidence level indicating that an IP address is the source of an attack is below a certain threshold (Nakae, paragraph 191). In other words, the threshold represents a likelihood that an IP address is causing an attack and not a total number of times that a server has been attacked, as claimed by the Applicants. Nakae does not teach reprovisioning (e.g., replacing) a server by instantiating a new server configuration, where the new server configuration is selected depending on the total number of times that the original server has been victim of an attack.

Gong similarly fails to teach or suggest selecting a specific remedy (e.g., new server configuration) based on a total number of times that a server has been attacked. Gong instead teaches a method in which new configurations for a network are automatically generated by an adaptive reconfigurer based on "tolerance objectives and any cost or performance impact" (Gong, column 7, lines 33-37).

Specifically, independent claim 1, as amended, recites:

1. A method for automated adaptive reprovisioning of servers under security assault, the method comprising:

PATENT

Atty. Dkt. No. YOR920030570US1

detecting a security assault or a possible security assault on a first server;
incrementing a counter that tracks a total number of times that the first server has been victim of a security assault or a possible security assault;
notifying a human operator if a value of said counter exceeds a maximum limit;
and

reprovisioning by automatically creating a new server instance with a new server configuration to perform at least one of the tasks performed by said first server, if said value of said counter does not exceed the maximum limit, wherein said new server configuration for said new server instance is selected from a table comprising a plurality of new server configurations, said new server configuration being associated in said table with said value of said counter such that a particular configuration of said new server configuration depends on the total number of times that said first server has been victim of a security assault.
(Emphasis added)

Applicants' invention is directed to a method and apparatus for adaptive server reprovisioning under security assault. When an assault on a server is detected, the server may be reconfigured in accordance with one of a number of potential new configurations designed to improve the server's resistance to subsequent assaults. These potential new configurations are stored in a table. Embodiments of the invention track (via a counter) a number of times that the server has been assaulted and use this number as an index into the table of potential new configurations, where at least one of the potential new configurations will correspond, according to the table, to the number of times that the given server has been assaulted. If the number of times that the server has been assaulted exceeds a predefined maximum number, a human operator is notified instead. In this way, a new configuration for the server can be selected automatically, based on the server's recorded vulnerability, and in a manner that minimizes server downtime and human intervention.

Applicants' independent claim 1, as amended, clearly recites the steps of incrementing a counter that tracks a total number of times that a first server has been victim of a security assault and automatically creating a new server instance with a new server configuration if the value of the counter does not exceed a maximum limit, where the new server configuration is selected from a table comprising a plurality of new server configurations, each of which is associated in the table with the value of the counter, such that a particular configuration of said new server configuration depends

PATENT

Atty. Dkt. No. YOR920030570US1

on the total number of times that the server has been victim of a security assault. As discussed above, Lachman in view of Nakae and further in view of Gong fails to teach or suggest these features. Accordingly, the Applicants respectfully submit that independent claim 1, as amended, is not made obvious by Lachman in view of Nakae and further in view of Gong and is patentable under 35 U.S.C. §103.

Claims 2-17 depend from claim 1 and recite additional features. As such, and at least for the same reasons set forth with respect to independent claim 1, the Applicants respectfully submit that claims 2-17 are also not made obvious by Lachman in view of Nakae and further in view of Gong and are patentable under 35 U.S.C. §103. Accordingly the Applicants respectfully request that the rejection of claims 1-17 under 35 U.S.C. §103 be withdrawn.

II. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

November 20, 2008

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702



Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404